



UNITED STATES PATENT AND TRADEMARK OFFICE

80
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/841,950	04/08/1997	MARK D. RIGGINS	40827.00004	3712

7590 01/26/2005

Jinntung Su
MANATT, PHELPS LLP
1001 Page Mill Road
Building 2
Palo Alto, CA 94203

EXAMINER

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 01/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

08/841,950

Applicant(s)

RIGGINS, MARK D.

Examiner

Thanhnga B. Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10/21/2004 (RCE).
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-6,8-14,16-20,22-30 and 32-39 is/are pending in the application.
- 4a) Of the above claim(s) 1,7,15,21 and 31 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-6,8-14,16-20,22-30 and 32-39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 2-6, 8-14, 16-20, 22-30, and 32-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogler (US 5,815,683), and further in view of Rosenow et. al. (US 5483596 A), Montague et. al. (US 5675782 A), Pilc et. al. (US 5510777 A) and Boyle et al. (US 5,872,847).

a. Referring to claim 6:

i. Vogler teaches:

(1) the limitations of a communication system linking client with web server is disclosed by Vogler Figure 1, elements 16 that is the Internet is the network that supports the world wide web). The further limitations, that security services are coupled to the web server, which determine access and authentication of the client determining client's remote privileges (Figure 2, element 18, 20, and 22) as well as enabling client to select among different (other) services (via a Browser (e.g. Netscape Navigator or later Column 4, lines 18-19)., figure 4 elements 44, 42, and 46, and Column 1, lines 37-40., column 4 lines 9-19) for example CAD tools communication services, etc, Column 1 , lines 37-40) is disclosed by Vogel. Vogel discloses one user authentication per request for service (for example a CAD problem) and is silent on presenting the user with a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it for authenticating the user according to at least one user authentication protocol. Montague, however, discloses presenting the user with a plurality of services for remote access and the use of user access rights with respect to applications which are controlled (Figure 2 and Column 3, lines 9-26). One of ordinary

skill in the art would have been motivated to combine the system of Vogler's with that of Montague because most users require flexibility especially in engineering designed, that is the use of CAD and expert program and with a number of services provided to the user, comes the need for access control and digital rights management. Vogler/Montague are silent on the issue for the need of additional authentication which may vary for the access required. Pilc et. al. disclose a system which uses additional authentication which depends on the level of additional security for the particular request (Column 2, lines 19-30). One of ordinary skill in the art would have been motivated to combine Vogler/Montague with the teachings of Pilc as the additional services of Montague would entail additional limitations of resources and security and this would be provided by Pilc. Vogler/Montague do not explicitly point out the option of the authentication protocol. Boyle teaches, authentication is a process of verifying the identity of a user, device, or other entity in the network. These processes may be implemented in the following ways: user identification; user authentication; dialog source authentication, wherein the source of all communication paths is authenticated at the receiving SNIU before communication is allowed; SNIU source authentication, wherein the source SNIU is authenticated before data is accepted for delivery; and administrator authentication, wherein an administrator is authenticated before being allowed access to the Security Manager functions (column 6, lines 52-64). One of ordinary skill in the art would have been motivated to combine the system of Vogler/Montague's with that of Boyle because most users require flexibility especially in engineering designed, that is the use of CAD and expert program and with a number of services provided to the user, comes the need for access control and digital rights management. Although Vogel's facilitator provides to the client service communications code that enables communication with a selected service (Figure 1, elements 14 (host engine), 12 and 10) Vogel is silent on whether these services are coupled to the security services or the use of keys stored in a secure memory (key safe) at the host that enable the client to access the available services without storing service communication codes and keys at the client. Rosenow provides a secure system for accessing files over a switched network for (figure 1, elements 46, 12, and 50 and figure

2), using resource authorization keys and access on the access controller (Figure 2, element 48 and Column 4, lines 47-55). Thus Rosenow authorization keys and resources are located at the server and would be of necessity held in a secure memory (key safe) at that site. Thus Rosenow when combined with Vogel would provide the details of security needed by Vogel. Although Vogel/Rosenow do not clearly disclose the key safe and its function, Boyle teaches, referring to Figure 1, elements 24 and 26 (key safe), the signature is validated and audited if necessary. If valid, the Association Manager 56 uses the Fortezza API to unwrap the sealer key(s). If two keys are in the received message, the bottom key is a release key to be shared with the first intermediate SNIU; and the top key is an association key to be shared with the peer SNIU (which granted the association). If there is only one key, it is the association key which is shared with the peer SNIU; and the association path does not contain any intermediate SNIUs. Once the keys are stored and the Association Table 76 is updated, the association is established and the Session Manager 48 is called to transmit the original user datagram which was stored in the waiting Queue prior to issuing the Association Request Message (column 9, lines 65-67 through column 10, lines 1-11). Thus Boyle when combined with Vogel would provide the details of security needed by Vogel.

b. Referring to claims 2-5:

i. Vogler/Montague/Pilc/Rosenow/Boyle further teaches:

(1) The limitations brought by claims 2 (SSL), 3 (encryption protocol), 4 (public key encryption) and 5 (public key certificates to authenticate) are well known methods for secure communications over a network and are well known in the cryptologic arts. One of ordinary skill in the art would have been motivated to combine Vogler/Montague/Pilc/Rosenow/Boyle, as necessary methods for implementing a secure network.

c. Referring to claims 8-14:

i. Vogler/Montague/Pilc/Rosenow/Boyle further teaches:

(1) the limitations of claims 11 (firewalls) and claim 14 (proxy) are well known in the network security arts and would be implemented on any

system which carried secure information across a network. Claim 8 relates to the determination of privileges of the user (see Column 3, lines 9-45 Montague), claims 10 the limitation of authentication information (Pilc, Column 2, lines 19-30) and the use of codes to negotiate devices claims 9, 12, 13, and 14 (see Rosenow Abstractl).

d. Referring to claims 16-19, 22-28:

i. These claims have limitations that is similar to those of claims 2-5 and 8-14, thus they are rejected with the same rationale applied against claims 2-5 and 8-14 above.

e. Referring to claim 20:

i. Claim 20 consist of a computer based method for implementing claim 6 and is rejected by the same prior art of record.

f. Referring to claim 29:

i. This claim recites a server computer system. Such variation are further disclosed by Vogel [i.e., Referring now to Figure 1, wherein a block diagram illustrating the networking topology of a CAD tool server, a plurality of clients, and an access facilitator facilitating the clients' access to the CAD tool server in accordance with the present invention is shown. For the illustrated embodiment, CAD tool server 10, clients 12, and access facilitator 14 are coupled to each other through Internet 16. Typically, though not necessarily, CAD tool server 10, clients 12, and access facilitator 14 are coupled to Internet 16 via Point of Presence providers; however, for ease of illustration, they are not shown. Additionally, CAD tool server 10 may also be coupled to access facilitator 14 via a local area network (LAN), and Internet 16 may be an organization's intranet. Alternatively, CAD tool server 10 and access facilitator 14 may reside on the same hardware (column 2, lines 63-67)].

ii. Vogler further teaches:

(1) the limitations of a communication system linking client with web server is disclosed by Vogler Figure 1, elements 16 that is the Internet is the network that supports the world wide web). The further limitations which determine access and authentication of the client determining client's remote privileges (Figure 2, element 18, 20, and 22) as well as enabling client to select among different (other)

Art Unit: 2135

services (via a Browser (e.g. Netscape Navigator or later Column 4, lines 18-19)., figure 4 elements 44, 42, and 46, and Column 1, lines 37-40., column 4 lines 9-19) for example CAD tools communication services, etc, Column 1 , lines 37-40) is disclosed by Vogel. Vogel discloses one user authentication per request for service (for example a CAD problem) and is silent on presenting the user with a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it for authenticating the user according to at least one user authentication protocol. Montague, however, discloses presenting the user with a plurality of services for remote access and the use of user access rights with respect to applications which are controlled (Figure 2 and Column 3, lines 9-26). One of ordinary skill in the art would have been motivated to combine the system of Vogler's with that of Montague because most users require flexibility especially in engineering designed, that is the use of CAD and expert program and with a number of services provided to the user, comes the need for access control and digital rights management. Vogler/Montague are silent on the issue for the need of additional authentication which may vary for the access required. Pilc et. al. disclose a system which uses additional authentication which depends on the level of additional security for the particular request (Column 2, lines 19-30). One of ordinary skill in the art would have been motivated to combine Vogler/Montague with the teachings of Pilc as the additional services of Montague would entail additional limitations of resources and security and this would be provided by Pilc. Vogler/Montague do not explicitly point out the option of the authentication protocol. Boyle teaches, authentication is a process of verifying the identity of a user, device, or other entity in the network. These processes may be implemented in the following ways: user identification; user authentication; dialog source authentication, wherein the source of all communication paths is authenticated at the receiving SNIU before communication is allowed; SNIU source authentication, wherein the source SNIU is authenticated before data is accepted for delivery; and administrator authentication, wherein an administrator is authenticated before being allowed access to the Security Manager functions (column 6, lines 52-64). One of ordinary skill in the art would have been motivated to combine the system of

Vogler/Montague's with that of Boyle because most users require flexibility especially in engineering designed, that is the use of CAD and expert program and with a number of services provided to the user, comes the need for access control and digital rights management. Although Vogel's facilitator provides to the client service communications code that enables communication with a selected service (Figure 1, elements 14 (host engine), 12 and 10) Vogel is silent on whether these services are coupled to the security services or the use of keys stored in a secure memory (key safe) at the host that enable the client to access the available services without storing service communication codes and keys at the client. Rosenow provides a secure system for accessing files over a switched network for (figure 1, elements 46, 12, and 50 and figure 2), using resource authorization keys and access on the access controller (Figure 2, element 48 and Column 4, lines 47-55). Thus Rosenow authorization keys and resources are located at the server and would be of necessity held in a secure memory (key safe) at that site. Thus Rosenow when combined with Vogel would provide the details of security needed by Vogel. Although Vogel/Rosenow do not clearly disclose the key safe and its function, Boyle teaches, referring to Figure 1, elements 24 and 26 (key safe), the signature is validated and audited if necessary. If valid, the Association Manager 56 uses the Fortezza API to unwrap the sealer key(s). If two keys are in the received message, the bottom key is a release key to be shared with the first intermediate SNIU; and the top key is an association key to be shared with the peer SNIU (which granted the association). If there is only one key, it is the association key which is shared with the peer SNIU; and the association path does not contain any intermediate SNIUs. Once the keys are stored and the Association Table 76 is updated, the association is established and the Session Manager 48 is called to transmit the original user datagram which was stored in the waiting Queue prior to issuing the Association Request Message (column 9, lines 65-67 through column 10, lines 1-11). Thus Boyle when combined with Vogel would provide the details of security needed by Vogel.

g. Referring to claim 30:

i. This claims have limitations that is similar to those of claims 6 and 29, thus it is rejected with the same rationale applied against claims 6 and 29 above.

h. Referring to claim 32:

i. This claim consist a method for receiving the data in an advanced communication and secured network to implement claim 6 and is rejected by the same prior art of record.

i. Referring to claims 33-36:

i. Rosenow further teaches:

(1) the association of keys with services and determination of client privileges using stored information (see especially Rosenow, claims 10-11).

j. Referring to claims 37, 38:

i. These claims have limitations that is similar to those of claim 32, thus they are rejected with the same rationale applied against claim 32 above.

k. Referring to claim 39:

i. This claim recites a server computer system (for communicating, security, access control and providing services) and web server (for presenting information to user) for implementing the system with the limitations recited in claim 6 and is rejected in view of the same prior art of record.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

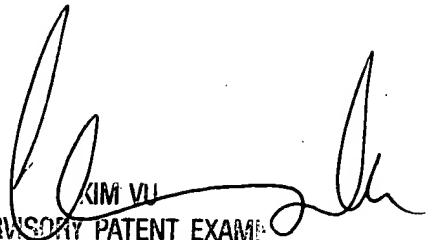
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2135

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

January 24, 2005



KIM V. L.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 21